

ABSTRACT

A person to be authenticated generates authentication data for this time and authentication data for next time using a one-way function, based on a user ID, a password and a random number, and performs an exclusive OR operation on these, to thereby encrypt the data while associating the both parameters with each other, and transmits these data together with the own user ID to an authenticating person. The authenticating person receives the aforesaid three informations, compares a validity confirmation parameter calculated by using a one-way function based on the authentication data for this time with a authentication parameter registered in the previous authentication phase, and when these parameters agree with each other, judges that authentication is approved, and registers the authentication data for next time as the authentication parameter for next time.

09766305-072401